Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

Claims 1.-12. (canceled).

Claim 13. (previously presented) A system for facilitating data management on a secure token, comprising:

a client having a plurality of applications residing thereon; and

a secure token having a storage architecture, wherein the storage architecture includes:

a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by the plurality of applications,

one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications, and

wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application;

wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application;

wherein the first set of operations is different from the second set of operations; and wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claims 14.-17. (canceled).

Claim 18. (previously presented) A system for facilitating data management on a secure token, comprising:

a client having a plurality of applications residing thereon; and

a secure token having a storage architecture, wherein the storage architecture includes:

a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by the plurality of applications,

one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the secure token is a smart card, ~~and~~

wherein the smart card is an open platform smart card, and

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 19. (canceled).

Claim 20. (previously presented) A secure token comprising:

a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client,

one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications,

wherein the one or more attributes associated with the cell group permit a first application to access that cell group after a first access condition is satisfied;

wherein the one or more attributes associated with the cell group permit a second application to access that cell group after a second access condition is satisfied;

wherein the first access condition is different from the second access condition,

and wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 21. (original) The secure token of claim 20 wherein the one or more attributes associated with the directory permit access to the directory by one application and deny access to the directory to another application.

Claim 22. (canceled).

Claim 23. (original) The secure token of claim 20 wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application.

Claim 24. (original) The secure token of claim 20 wherein one or more additional cell groups are added to the directory subsequent to issuance of the secure token to a token holder.

Claim 25. (original) The secure token of claim 20 wherein ownership of one of the one or more cell groups is determined subsequent to issuance of the secure token to a token holder.

Claim 26. (original) The secure token of claim 20 wherein ownership of one of the one or more cell groups is modified subsequent to issuance of the secure token to a token holder.

Claim 27. (original) The secure token of claim 20 wherein one or more additional cells are added to a cell group subsequent to issuance of the secure token to a token holder.

Claim 28. (original) The secure token of claim 20

wherein the one or more attributes associated with the directory are modified in terms of permitting or denying access to the directory by the plurality of applications.

Claim 29. (canceled)

Claim 30. (original) The secure token of claim 20

wherein the one or more attributes associated with a cell are modified in terms of permitting or denying access to that cell by the plurality of applications.

Claim 31. (original) The secure token of claim 20 wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications.

Claim 32. (previously presented) A secure token comprising:

a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client terminal,

one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications,

wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application;

wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application; and

wherein the first set of operations is different from the second set of operations, and

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client terminal is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 33. (original) The secure token of claim 20 wherein the one or more attributes associated with the directory permit a first application to access the directory after a first access condition is satisfied;

wherein the one or more attributes associated with the directory permit a second application to access the directory after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition.

Claim 34. (canceled).

Claim 35. (original) The secure token of claim 20 wherein the one or more attributes associated with the cell permit a first application to access that cell after a first access condition is satisfied;

wherein the one or more attributes associated with the cell permit a second application to access that cell after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition.

Claim 36. (original). The secure token of claim 20 wherein the secure token is a smart card.

Claim 37. (previously presented) A secure token comprising:

a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client,

one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the secure token is a smart card, and wherein the smart card is an open platform smart card,

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 38. (original) The secure token of claim 36 wherein the smart card is a static or native smart card.

Claim 39. (previously presented) A method for facilitating data management on a secure token, comprising:

providing a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client,

providing one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

providing one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications,

wherein the one or more attributes associated with the cell group permit a first application to access that cell group after a first access condition is satisfied;

wherein the one or more attributes associated with the cell group permit a second application to access that cell group after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition, and

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 40. (original) The method of claim 39 wherein the one or more attributes associated with the directory permit access to the directory by one application and deny access to the directory to another application.

Claim 41. (canceled).

Claim 42. (original) The method of claim 39 wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application.

Claim 43. (original) The method of claim 39 further comprising:

adding one or more additional cell groups to the directory subsequent to issuance of the secure token to a token holder.

Claim 44. (original) The method of claim 39 further comprising:

determining ownership of one of the one or more cell groups subsequent to issuance of the secure token to a token holder.

Claim 45. (original) The method of claim 39 further comprising:

modifying ownership of one of the one or more cell groups subsequent to issuance of the secure token to a token holder.

Claim 46. (original) The method of claim 39 further comprising:

adding one or more additional cells to a cell group subsequent to issuance of the secure token to a token holder.

Claim 47. (original) The method of claim 39 further comprising:

modifying the one or more attributes associated with the directory in terms of permitting or denying access to the directory by the plurality of applications.

Claim 48. (original) The method of claim 39 further comprising:

modifying the one or more attributes associated with a cell group in terms of permitting or denying access to that cell group by the plurality of applications.

Claim 49. (original) The method of claim 39 further comprising:

modifying the one or more attributes associated with a cell in terms of permitting or denying access to that cell by the plurality of applications.

Claim 50. (original) The method of claim 39 wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications.

Claim 51. (original) The method of claim 50 wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application;

wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application; and

wherein the first set of operations is different from the second set of operations.

Claim 52. (original) The method of claim 39 wherein the one or more attributes associated with the directory permit a first application to access the directory after a first access condition is satisfied;

wherein the one or more attributes associated with the directory permit a second application to access the directory after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition.

Claim 53. (canceled).

Claim 54. (original) The method of claim 39 wherein the one or more attributes associated with the cell permit a first application to access that cell after a first access condition is satisfied;

wherein the one or more attributes associated with the cell permit a second application to access that cell after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition.

Claim 55. (original) The method of claim 39 wherein the secure token is a smart card.

Claim 56. (previously presented) A method for facilitating data management on a secure token, comprising:

providing a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client,

providing one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

providing one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications, wherein the secured token is a smart card and wherein the smart card is an open platform smart card, and

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Claim 57. (original) The method of claim 55 wherein the smart card is a static or native smart card.

Claim 58. (previously presented) The method of claim 39 wherein the first application is associated with a first party and the second application is associated with a second party, and wherein the first party and the second party have an existing business relationship and agree to share data on the secure token according to agreed security controls.

Claim 59. (previously presented) The method of claim 58 wherein the first application or the second application is a loyalty application.

Claim 60. (previously presented) The method of claim 59 wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups.

Claim 61. (previously presented) The secure token of claim 32 wherein the first application is associated with a first party and the second application is associated with a second party, and wherein the first party and the second party have an existing business relationship and agree to share data on the secure token according to agreed security controls.